Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

Invariantive Theory of Plane Cubic Curves Modulo 2.

By L. E. Dickson.

§ 1. *Introduction.*

The ten types of plane cubic curves in ordinary geometry have been characterized by invariants and covariants by Gordan.[*] The types in modular geometry can be characterized by invariants only, the abundance of invariants making it unnecessary to resort to covariants. The most effective theory of modular invariants is that based upon a separation of the particular cases of the form in question into classes of equivalent forms.

For the present problem of cubic curves modulo 2, this classification is effected in § 3 by means of the real points (*i. e.*, points with integral coördinates) on the cubic, supplemented by a determination of the real inflexion points and the real and imaginary singular points. While we could test directly each real point on the curve, not a singular point, and find whether or not it is an inflexion point, we have completed the geometrical investigation by making a determination of all of the real and imaginary inflexion points on each of the twenty-two types of cubic curves modulo 2. For this purpose we have set up in § 2 a cubic function *H*, which here plays a rôle analogous to that played by the Hessian in the algebraic theory.

From the geometrical classification of the modular cubics we easily derive in § 4 a fundamental system of modular invariants.

The methods employed in this paper are applicable to other problems of this nature; they indicate the decided advantage to be gained in the theory of modular invariants from modular geometry as developed by Bussey and Veblen, Coble and the writer.

§ 2. *Inflexion Points on Cubic Curves.*

Let there be a single intersection of

$$x_3 = ax_1 + bx_2 \tag{1}$$

with the cubic $u(x_1, x_2, x_3) = 0$. Then

$$u(x_1, x_2, ax_1 + bx_2) = U(x_1, x_2) = \alpha x_1^3 + \beta x_1^2 x_2 + \gamma x_1 x_2^2 + \delta x_2^3 \tag{2}$$

---

[*] *Transactions Amer. Math. Soc.*, Vol. I (1900), p. 402.

is the cube, modulo 2, of $\alpha x_1+\delta x_2$, so that $\beta\equiv\gamma\equiv\alpha\delta$. Thus the point on (1) with $x_1=\delta$, $x_2=\alpha$, is an inflexion point. For these values,

$$\tfrac{1}{2}\frac{\partial^2 U}{\partial x_1^2}=3\alpha x_1+\beta x_2,\quad \tfrac{1}{2}\frac{\partial^2 U}{\partial x_1\partial x_2}=\beta x_1+\gamma x_2,\quad \tfrac{1}{2}\frac{\partial^2 U}{\partial x_2^2}=\gamma x_1+3\delta x_2$$

all reduce to zero modulo 2. By (2),

$$\frac{\partial^2 U}{\partial x_1^2}=\frac{\partial^2 u}{\partial x_1^2}+2a\frac{\partial^2 u}{\partial x_1\partial x_3}+a^2\frac{\partial^2 u}{\partial x_3^2},\quad \frac{\partial^2 U}{\partial x_2^2}=\frac{\partial^2 u}{\partial x_2^2}+2b\frac{\partial^2 u}{\partial x_2\partial x_3}+b^2\frac{\partial^2 u}{\partial x_3^2},$$

$$\frac{\partial^2 U}{\partial x_1\partial x_2}=\frac{\partial^2 u}{\partial x_1\partial x_2}+b\frac{\partial^2 u}{\partial x_1\partial x_3}+a\frac{\partial^2 u}{\partial x_2\partial x_3}+ab\frac{\partial^2 u}{\partial x_3^2}.$$

For each derivative in the second members, every term has an even coefficient except the term derived from $x_1x_2x_3$. We set

$$u=v+kx_1x_2x_3,\quad \xi_i=\tfrac{1}{2}\frac{\partial^2 v}{\partial x_i^2},\quad \eta_1=\tfrac{1}{2}\frac{\partial^2 v}{\partial x_2\partial x_3},\quad \cdots\cdots \tag{3}$$

Thus, at our inflexion point,

$$\xi_1+akx_2+a^2\xi_3\equiv 0,\quad \xi_2+bkx_1+b^2\xi_3\equiv 0, \tag{4}$$

$$\eta_3+b\eta_2+a\eta_1+ab\xi_3+kx_3\equiv 0 \pmod 2. \tag{5}$$

Multiply (4_1) by x_1^2, (4_2) by x_2^2, add and apply (1). We get

$$\xi_1x_1^2+\xi_2x_2^2+\xi_3x_3^2+kx_1x_2x_3\equiv 0. \tag{6}$$

This is equivalent modulo 2 to $u\equiv 0$. We therefore drop (4_1).

Eliminating a between (1) and (5), and then b between the resulting congruence and (4_2), we find, after simplifications by use of (6) and a final deletion of the factor x_1^2, that

$$H=\xi_1\xi_2\xi_3+\Sigma\xi_i\eta_i^2+k\Sigma x_i\xi_i\eta_i+k\Sigma x_1\eta_2\eta_3+k^2\Sigma x_1x_2\eta_3+k^3x_1x_2x_3\equiv 0. \tag{7}$$

Evidently H is a covariant of u with respect to any interchange of variables.* Let $x_1=x_1'+x_2'$, $x_2=x_2'$, $x_3=x_3'$ replace u by u', and let c be the coefficient of $x_1^2x_3$ in u. If we form the function H for u' (*i. e.*, for the transformed variables and coefficients), we find that it equals $H+(c^2+kc)u$ modulo 2, formally in the initial variables and coefficients. Hence, *the system of equations $u=0$, $H=0$ is invariant under every linear transformation with integral coefficients modulo* 2.

Thus the inflexion and singular points of $u=0$ are given by its intersections with $H=0$, so that H here plays a rôle analogous to that of the Hessian in the theory of algebraic curves.

---

[*] Hence it was no restriction to take the coefficient of x_3 in (1) to be not zero.

§ 3. *Cubic Curves Classified Geometrically.*

We shall find that two cubic curves with integral coefficients modulo 2 are equivalent under the group G of all linear transformations with integral coefficients modulo 2 if and only if they have the same number of real points, real inflexion points and real or imaginary singular points. In § 4, we deduce criteria by invariants.

The seven real points modulo 2 shall be designated

$$1=(100),\ 2=(010),\ 3=(001),\ 4=(110),\ 5=(101),\ 6=(011),\ 7=(111).$$

At these points the values of

$$C=ax^3+by^3+cz^3+dx^2y+exy^2+fx^2z+gxz^2+hy^2z+iyz^2+jxyz$$

are respectively

$$a,\ b,\ c,\ a+b+d+e,\ a+c+f+g,\ b+c+h+i,\ s, \tag{8}$$

where s is the sum of the ten coefficients of C. Denote by C_r a form C for which $C\equiv 0 \pmod 2$ contains exactly r real points.

Case $r=0$. Each function (8) is unity modulo 2, whence

$$C=x^3+y^3+z^3+dx^2y+(d+1)xy^2+fx^2z+(f+1)xz^2+hy^2z+(h+1)yz^2+xyz.$$

Replacing x by $x+dy+fz$, we get a C with $d=f=0$. Then replacing y by $y+hz$, we have also $h=0$ and get

$$C_0=x^3+y^3+z^3+xy^2+xz^2+yz^2+xyz, \quad H=C_0. \tag{I}$$

Its singular points are $(1, z^2, z)$, where $z^3+z+1\equiv 0$ is irreducible modulo 2. It can be shown that C_0 is the product of three imaginary linear functions.

Case $r=1$. After applying a transformation of G, we have a C the only real point on which is 1. In fact, $1=(100)$ is transformed into (α, β, γ) by the linear transformation having α, β, γ as the coefficients of x in x', y', z'. Thus $a=0$, while the remaining functions (8) are unity, so that

$$C=y^3+z^3+d(x^2y+xy^2)+f(x^2z+xz^2)+hy^2z+(h+1)yz^2.$$

The transformations leaving point 1 fixed are

$$x'=x+ry+tz, \quad y'=\alpha y+\beta z, \quad z'=\gamma y+\delta z. \tag{9}$$

By the interchange of y and z, d and f are permuted, while h is replaced by $h+1$. For $y'=y+z$, we get $f'=f+d$, $h'=h+1$. Unless $d=f=0$, we may therefore set $d=1$, $f=0$; then, replacing x by $x+hz$, we have also $h=0$ and get

$$C_1=y^3+z^3+x^2y+xy^2+yz^2, \quad H=x^2y+xy^2+x^2z+yz^2+xyz. \tag{II}$$

To eliminate x, note that

$$y(C_1+H)+zC_1\equiv y^4+y^3z+z^4 \pmod{2}.$$

The nine inflexion points* are $1=(100)$ and $(\xi, 1, \zeta)$, where

$$\zeta^4+\zeta+1\equiv 0, \quad \xi^2+\xi+\zeta^3+\zeta^2+1\equiv 0,$$

of which the first is irreducible modulo 2, while the second has no root rational in ζ, since $\xi^{16}+\xi\equiv 1$. The coördinates of the eight imaginary inflexion points are in the Galois field of order 2^8. There is no singular point.

If $d=f=0$, we may set $h=0$, after interchanging y and z when necessary, and get

$$C_1'=y^3+z^3+yz^2, \quad H\equiv 0. \tag{III}$$

This binary form represents three intersecting imaginary lines. The point 1 is the only singular point.

Case $r=2$. Since (9) replaces (010) by (r, α, γ), where α and γ are not both zero, any pair of real points can be transformed into the pair 1, 2. If the latter are the only real points on it, the cubic is

$$C=z^3+dx^2y+(d+1)xy^2+f(x^2z+xz^2)+h(y^2z+yz^2)+xyz.$$

After interchanging x and y if necessary, we may set $d=0$. Then replacing x by $x+hz$, we have also $h=0$, and get

$$C_2=z^3+xy^2+x^2z+xz^2+xyz, \quad H=x^3+xz^2+y^2z+yz^2; \tag{IV}$$

$$C_2'=z^3+xy^2+xyz, \quad H=xy^2+y^2z+yz^2+xyz. \tag{V}$$

The nine inflexion points of C_2 are (010), $(x, y, 1)$, where

$$x^4+x+1\equiv 0, \quad y^2+y\equiv x^3+x.$$

There is no singular point. Since

$$C_2'+H\equiv z(y^2+yz+z^2),$$

the three inflexion points of C_2' are (010), $(1, y, 1)$, where $y^2+y+1\equiv 0$, while the only singular point is (100).

Case $r=3$. As two of the points we may take 1 and 2. First, let the third real point on C be 4, the only real point collinear with 1 and 2. Then

$$C=z^3+d(x^2y+xy^2)+f(x^2z+xz^2)+h(y^2z+yz^2).$$

---

* The imaginary ones are determined for the sake of completeness; but a knowledge of them is not essential for our present purposes.

If $d=1$, replace x by $x+hz$ and y by $y+fz$ to make $f=h=0$:

$$C_3=z^3+x^2y+xy^2, \quad H=(x^2+y^2+xy)z. \tag{VI}$$

There is no singular point. The nine inflexion points are 1, 2, 4, $(k, 1, 1)$, $(1, k, 1)$, $(k+1, k, 1)$, where $k^2+k+1\equiv 0$. If $d=f=h=0$, we have

$$C_3'=z^3, \quad H\equiv 0. \tag{VII}$$

The only singular points are (100), $(\alpha, 1, 0)$. If $d=0$, while f and h are not both zero, we may set $f=1$ after interchanging x and y when necessary. Replacing x by $x+hy$, we have also $h=0$ and get the binary form

$$C_3''=z^3+x^2z+xz^2, \quad H\equiv 0, \tag{VIII}$$

with the single singular point 2.

Second, let the three real points on C be 1, 2 and a point not collinear with them and hence having $z=1$. Since

$$x'=x+cz, \quad y'=y+sz, \quad z'=z \tag{10}$$

leaves 1 and 2 fixed and replaces 3 by $(c, s, 1)$, we can transform the three real points into 1, 2, 3. Thus

$$C=dx^2y+(d+1)xy^2+fx^2z+(f+1)xz^2+hy^2z+(h+1)yz^2. \tag{11}$$

Interchanging x and y if necessary, we may set $d=0$. If $f=h=1$, the substitution (x, y, z) replaces C by a similar C with $d=f=h=0$. If $f=1$, $h=0$, we have

$$K_3=xy^2+x^2z+yz^2, \quad H=x^3+y^3+z^3+xyz. \tag{IX}$$

Eliminating x^3 and then x^2, we get $xy^4=z^5$. We see that the inflexion points are $(z^5, 1, z)$, where $z^9+z^3+1=0$, with the irreducible factors z^3+z^2+1, $z^6+z^5+z^4+z^2+1$. But if $f=0$, we may set $h=0$, after interchanging y and z if necessary, and get

$$K_3'=xy^2+xz^2+yz^2, \quad H=xz^2+xy^2+y^3. \tag{X}$$

They intersect in just two points, the singular point 1 and inflexion point 3.

Case $r=4$. The three real points not on $C=0$ may be taken, as in case $r=3$, to be any three collinear points, as 4, 5, 6; or any three non-collinear points, as 5, 6, 7.

In the first case, the only real points on C are 1, 2, 3, 7, and C is $C'+xyz$, where C' is given by (11). Since the normalizations of C' were effected by permutations of the variables, we have merely to add xyz to the canonical forms (IX) and (X) to get provisional canonical forms $K_4=K_3+xyz$ and K'_3+xyz. But $y'=y+x$, $z'=z+x$ replaces the latter by the former:

$$K_4=xy^2+x^2z+yz^2+xyz, \quad H=x^3+y^3+z^3+xy^2+x^2z+yz^2. \tag{XI}$$

The sum of the two is

$$x^3+y^3+z^3+xyz\equiv(x+y+z)\,(x+\omega y+\omega^2z)\,(x+\omega^2y+\omega z),$$

where $\omega^2+\omega+1\equiv 0 \pmod 2$. If the first factor is zero, we get the three inflexion points $(z+1, 1, z)$, where $z^3+z+1=0$. If the second factor is zero, K_4 becomes, after x is eliminated, $\omega(y+z)^3$. To treat the third factor, we have only to replace ω by ω^2. In each of the latter cases we obtain the unique singular point (111).

In the second main case, the only real points on C are 1, 2, 3, 4. Thus

$$C=d(x^2y+xy^2)+fx^2z+(f+1)xz^2+hy^2z+(h+1)yz^2+xyz.$$

For $f=h=0$, C is transformed into a like C with $f=1$, $h=0$, by replacing y by $x+y$. The new C is transformed into one with $f=0$, $h=1$ by (xy). Hence we may set $f=h$ and obtain the four types

$$C_4=xz^2+yz^2+xyz, \quad H=C_4+z^3; \tag{XII}$$

$$C'_4=C_4+x^2y+xy^2, \quad H=x^3+y^3+z^3+x^2y+xy^2+xyz; \tag{XIII}$$

$$C''_4=x^2z+y^2z+xyz, \quad H\equiv 0; \tag{XIV}$$

$$C'''_4=C''_4+x^2y+xy^2, \quad H=x^2y+xy^2. \tag{XV}$$

The only singular points of C_4 are 1 and 2. There is no singular point on C'_4; for $z=0$, H vanishes only at (110), an inflexion point; for $z\neq 0$, we obtain the eight imaginary inflexion points $(x, y, 1)$, where

$$y^8+y^7+y^6+y^5+y^2+y+1\equiv 0, \quad x=\frac{y^5+y}{y^4+y^2+1},$$

the congruence in y being irreducible modulo 2. The singular points on C''_4 are 3 and $(1, k, 0)$, $k^2+k+1\equiv 0 \pmod 2$. The only singular point on C'''_4 is 3; the only inflexion points are 1, 2, 4.

Case $r=5$. The real points not on C may be taken to be 1, 2. Then

$$C=x^3+y^3+d(x^2y+xy^2)+fx^2z+(f+1)xz^2+hy^2z+(h+1)yz^2.$$

It is transformed by (10) into one with

$$f'=f+c+ds, \quad h'=h+s+dc.$$

If $d=0$, we take $c=f$, $s=h$, and have $f'=h'=0$. Then

$$C=x^3+y^3+xz^2+yz^2.$$

Replacing x by $x+y$ and z by $x+y+z$, we get

$$C_5=x(xy+z^2), \quad H=x^3. \tag{XVI}$$

The only singular point is 2. Next, let $d=1$; we take $s=0$, $c=f$ and have $f'=0$. If $h=0$, $C=(x+y)(x^2+y^2+z^2)$; replacing x by $x+y$ and z by $z+x$, we get

$$C'_5=xz^2, \quad H\equiv 0, \tag{XVII}$$

and see that any point with $z=0$ is singular. If $h=1$,

$$C=(x+y)^3+xz^2+y^2z.$$

Replacing x by $x+y$, we get

$$C''_5=x^3+(x+y)z^2+y^2z, \quad H=z^3+xy^2+xz^2+x^2z+xyz. \tag{XVIII}$$

Since $xC''_5+zH=x^4+xz^3+z^4$, the nine inflexion points are (010) and $(x, y, 1)$, where $x^4+x+1=0$, $y^2+y=x^3+x$. From the square of the latter we get $x=y^4+y$, whence $y^8+y^6+y^5+y^4+y^3+y+1\equiv 0$, which is irreducible modulo 2.

Case $r=6$. Let 7 be the real point not on C. Then

$$C=d(x^2y+xy^2)+f(x^2z+xz^2)+h(y^2z+yz^2)+xyz. \tag{12}$$

Replacing x by $x+y+z$, we get a C with $h'=h+d+f+1$. Again, any two of the coefficients d, f, h are interchanged by a suitably chosen interchange of the variables. Hence, if two of the coefficients are zero, we may set $d=f=0$; then either h itself is zero or else h' is zero, and we get

$$C_6=xyz=H, \tag{XIX}$$

with the singular points 1, 2, 3.

If every coefficient is unity, then $h'=0$. Thus there remains only the case in which just one coefficient is zero. We may then take $d=0$, $f=h=1$; replacing x by $x+z$, we get

$$C_6'=z(x^2+xz+y^2+xy), \quad H=z^3. \tag{XX}$$

The singular points are $(1, k, 0)$, where $k^2+k+1\equiv 0$.

Case $r=7$. We have (12) without the term xyz. If the cubic is not identically zero, we may set $f=1$. Replacing x by $x+hy$, we have $f=1$, $h=0$. Replacing z by $z+dy$, we get

$$C_7=x^2z+xz^2, \quad H\equiv 0. \tag{XXI}$$

The only singular point is 2.

§ 4. *Classification by Invariants.*

Since the transformations of our group G permute the real points $1, \ldots, 7$, they permute the values (8). Hence any symmetric function of $a, \ldots, s$ is a formal invariant of C modulo 2. In particular, their elementary symmetric function E_k of degree k is an invariant. The value of E_1 is the coefficient of xyz.

Denote by C_r a form C for which the cubic curve $C\equiv 0 \pmod 2$ contains exactly r real points. For a C_r, exactly $7-r$ of the values $a, \ldots, s$ are unity and the others are zero. Thus $E_k=1$ or 0, according as $k=7-r$ or $k>7-r$. We may therefore employ the rational integral invariants E_k to show that a C_r and a C_r' are not equivalent under the group G if $r\neq r'$.

For a real point (x, y, z), the product

$$P=\left(1+\frac{\partial C}{\partial x}\right)\left(1+\frac{\partial C}{\partial y}\right)\left(1+\frac{\partial C}{\partial z}\right)$$

has the value 1 or 0 modulo 2, according as the point is or is not a singular point. Let ε_k be the elementary symmetric function of order k of the values of P at the seven real points. For a cubic with s real singular points, s of the values of P are unity and the other values are zero, so that $\varepsilon_s=1$, $\varepsilon_k=0\ (k>s)$, for this cubic. We may therefore use the rational integral invariants ε_k to show that two cubics are not equivalent under G if the numbers of their real singular points are different.

To account for the total number of real singular and inflexion points, we may make a similar use of the symmetric functions of the values of $(1+C)(1+H)$ at the seven real points.

Corresponding formal invariants of C may be found by employing, in place of the real points, the points whose coördinates are in the Galois field of a given order 2^n.

The twenty-two classes of cubic curves under G, including the cubic which is identically zero, can therefore be characterized by rational integral invariants of the preceding types. In view of a general theorem (Madison Colloquium Lectures, 1914, p. 14), these invariants form a fundamental system of modular invariants of C modulo 2.

§ 5. *Classes of Cubic Curves under Imaginary Transformations.*

In what follows, let $a^3+a+1=0$, $b^2+b+1=0$. Then C_0 has the three factors $x+ay+a^2z$ and is equivalent to C_6. The latter is true of C_4'', with the factors z, $x+by$, $x+b^2y$. From C_7 written in capitals, we obtain C_3'' by setting $X=x+bz$, $Z=x+b^2z$, whence $X+Z=z$; while we obtain C_1' by setting $X=ay+a^2z$, $Z=a^2y+a^4z$, whence $X+Z=a^4y+az$.

We pass to the curves C for which C and H are linearly independent. The two real types having only two singular points are C_4 and C_6'. The latter written in capitals becomes C_4 if $X=x+y$, $Y=kx+k^2y$, $Z=z$. Of the five real types with one singular point, C_5 has no inflexion point (being a conic and a tangent), K_3' has a single inflexion, while C_2', K_4 and C_4''' have three inflexions. Now C_2' in capitals becomes C_4''' if $X=x+z$, $Y=bx+y$, $Z=x$, and K_4 in capitals becomes C_4''' if

$$X=ax+a^2y+z,\quad Y=a^2x+(a+a^2)y+z,\quad Z=(a+a^2)x+ay+z.$$

There remain six real types with nine inflexions; of these, C_1, C_3, K_3 and C_5'' have no xyz term and are equivalent to $\sigma=X^3+Y^3+Z^3$ (for example, C_3 becomes σ if $x=Y+Z$, $y=X+Y$, $z=X+Y+Z$); while C_2 and C_4' have such a term and are equivalent to $\sigma+tXYZ$, where $t \neq 0$. Note that the coefficient of xyz in the general cubic C is a relative invariant of C modulo 2.

The resulting ten types under imaginary transformations are seen to be in complete accord with the ten of Gordan, after his coefficient 6 is deleted. Our last two types are his C_1, C_2. His C_3 is X^3+Y^3+XYZ and becomes our

C_2' for $X=y$, $Y=y+z$, $Z=x+z$. His C_4 is Z^3+XYZ and becomes our C_4 for $X=x+z$, $Y=y+z$, $Z=z$. His C_6 is XY^2+Z^3 and becomes our K_3' for $X=x+y$, $Y=y+z$, $Z=y$. His C_8 is equivalent to $(z+x)^3+x^3=C_3''$. His C_5, C_7, C_9, C_{10} are our C_6, C_5, C_5', C_3', respectively.

Although we might derive this list of ten types independently of the longer list of real types, it would be difficult to deduce therefrom the classes of real cubics under real transformation.

UNIVERSITY OF CHICAGO, *July*, 1914.